

AMENDMENTS TO THE CLAIMS

1. (Currently amended): An updating system for an encrypted key for a wireless LAN in which ~~a one or more~~ wireless access point ~~is~~ points (APs) ~~are~~ provided on a LAN, said wireless access point ~~AP's~~ being wirelessly connected to a plurality of one or more wireless access terminal devices (STAs) and in which data is encrypted and transmitted between the wireless access point ~~AP or APs~~ and the plurality of wireless access terminal devices, STA or STAs to effect communication ~~(encrypted communication)~~; said system comprising:

a key management server ~~(SV) device, said key management server (SV) device, LAN-connected to said wireless access point~~ the AP, comprising:

a SV storage unit for holding k encrypted keys used in the encrypted communication between said wireless access point ~~AP or APs~~ and the plurality of wireless access terminal devices ~~STA or STAs~~, where k is not less than 1; and

an encrypted key generating unit generating said k encrypted keys ~~key~~ and storing the generated k encrypted keys ~~key~~ in said SV-storage unit;

wherein said key management server ~~SV device~~ generating said encrypted key in said encrypted key generating unit to store the generated encrypted key in said SV storage unit, said SV device ~~control~~ controlling said encrypted key generating unit to update one of said encrypted key ~~keys~~ stored in said SV-storage unit and deliver ~~to deliver~~ the updated encrypted key to said wireless access point ~~AP~~ and to said plurality of wireless access terminal devices ~~STA or STAs~~.

2. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 1 wherein:

upon updating said encrypted key stored in said ~~SV~~-storage unit, said key management server~~SV~~ device generates and updates a sole encrypted key at a time by said encrypted key generating unit.

3. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 1 wherein:

upon updating said encrypted key stored in said ~~SV~~-storage unit, said key management server~~SV~~ device generates a sole encrypted key at a time by said encrypted key generating unit and sequentially updates k encrypted keys stored in said ~~SV~~-storage unit one-by-one at a preset interval.

4. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 1 wherein:

where k is greater than 1, said key management server~~SV~~ device sequentially updates all except a remaining one~~(k-1)~~ of said k encrypted keys stored in said ~~SV~~-storage unit one-by-one at a preset first interval, said key management server~~SV~~ device updating the remaining one key at a second interval which is longer than said preset first interval~~that for said (k-1) encrypted keys~~.

5. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 2 wherein:

said wireless access point~~AP~~ comprises an updating unit updating an nth encrypted key, stored and managed by said wireless access point~~AP~~ or APs, on reception of a delivered nth encrypted key updated by said key management server~~SV~~ device, where  $1 \leq n \leq k$ , and where k is greater

than 1, and an encryption unit encrypting an encrypted key updating notification message, using an encrypted key other than said nth encrypted key, ~~for advising said STA or STAs of that effect;~~

each of said plurality of wireless access terminal devicesSTA comprising a key generating unit generating an STA-encrypted key updating requesting message on reception of said encrypted key updating notification message from said wireless access pointAP and an encryption unit encrypting said STA-encrypted key updating requesting message, using the same encrypted key as that used in said encrypted key updating notification message, ~~to advise said AP of that effect; and~~

said wireless access pointAP also comprising a transmission unit advising said key management serverSV device of the STA-encrypted key updating ~~request on~~ reception of said STA-encrypted key updating requesting message ~~from said STA;~~

said key management serverSV device also comprising a verification unit verifying whether or not an encrypted key may be delivered to one of said plurality of wireless access terminal devicesSTA on reception of the STA encrypted key updating requesting message from said wireless access pointAP, and a delivery unit that delivers, if such verification is true, delivering to said wireless access pointAP the encrypted key addressed to said one of said plurality of wireless access terminal devicesSTA ~~if it is verified that said encrypted key may be delivered to said STA.~~

6. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 2 wherein:

said wireless access pointAP comprises an updating unit updating an nth encrypted key, stored and managed by said wireless access pointAP or APs, on reception of a delivered nth encrypted key updated by said key management server deviceSV, where  $1 \leq n \leq k$ , and an encryption unit encrypting an encrypted key updating notification message, using an initially updated one of k encrypted keys stored and managed by said wireless access pointAP, ~~to advise said STA of that effect;~~

each of said plurality of wireless access terminal devicesSTA comprising a generator unit generating an ~~STA-encrypted~~ key updating requesting message on reception of said encrypted key updating notification message from said wireless access pointAP and an encryption unit encrypting said ~~STA-encrypted~~ key updating requesting message, using the same encrypted key as that used ~~to encrypt~~ said encrypted key updating notification message, ~~to advise said AP of that effect;~~

said wireless access pointAP also comprising a transmission unit advising said key management serverSV device of the ~~STA-encrypted key updating request~~ on reception of said ~~STA-encrypted~~ key updating requesting message ~~from said STA;~~

said key management serverSV device also comprising a verification unit verifying whether or not an encrypted key may be delivered to one of said plurality of wireless access terminal devicesSTA on reception of the STA encrypted key updating requesting message from said wireless access pointAP and a delivery unit that delivers, if such verification is true, delivering to said wireless access pointAP the encrypted key addressed to said one of said plurality of wireless access terminal devicesSTA ~~if it is verified that said encrypted key may be delivered to said STA.~~

7. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 5 wherein

said wireless access point~~AP~~ comprises a generator unit generating an ~~STA~~ encrypted key delivery message on reception of an encrypted key addressed to said one of said plurality of wireless access terminal devices~~STA~~ from said key management server~~SV~~ device; and an encryption unit encrypting said ~~STA~~-encrypted key delivery message, using an encrypted key other than the nth encrypted key, ~~to advise said STA of that effect;~~

said one of said plurality of wireless access terminal devices~~STA~~ also comprising an updating unit updating an nth encrypted key stored and managed by said one of said plurality of wireless access terminal devices~~STA~~ on reception of an nth encrypted key by said ~~STA~~-encrypted key delivery message from said wireless access point~~AP~~.

8. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 6 wherein

said ~~AP~~wireless access point comprises a generator unit generating an ~~STA~~ encrypted key delivery message on reception of an encrypted key addressed to said ~~STA~~one of said plurality of wireless access terminal devices from said ~~SV~~key management server device; and an encryption unit encrypting said ~~STA~~-encrypted key delivery message, using an encrypted key other than the nth encrypted key, ~~to advise said STA of that effect;~~

said ~~STA~~one of said plurality of wireless access terminal devices also comprising an updating unit updating an nth encrypted key stored and managed by

said ~~STA~~one of said plurality of wireless access terminal devices on reception of ~~said an~~ nth encrypted key by said ~~STA~~-encrypted key delivery message from said ~~AP~~wireless access point.

9. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 5 wherein:

said ~~AP~~wireless access point comprises a generator unit generating an ~~STA~~-encrypted key delivery message on reception of an encrypted key addressed to said ~~STA~~one of said plurality of wireless access terminal devices from said ~~SV~~key management server device, and

an encryption unit encrypting said ~~STA~~-encrypted key delivery message, using an initially updated one of k encrypted keys stored and managed by said ~~AP~~wireless access point, ~~to advise said STA of that effect;~~

said ~~STA~~one of said plurality of wireless access terminal devices also comprising an updating unit updating an nth encrypted key stored and managed by said ~~STA~~one of said plurality of wireless access terminal devices on reception of an nth encrypted key by delivered said ~~STA~~-encrypted key delivery message from said ~~AP~~wireless access point.

10. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 6 wherein:

said ~~AP~~wireless access point comprises:

a generator unit generating an ~~STA~~-encrypted key delivery message on reception of an encrypted key addressed to said ~~STA~~one of said plurality of wireless access terminal devices from said ~~SV~~key management server device,; and

an encryption unit encrypting said ~~STA~~-encrypted key delivery message, using an initially updated one of k encrypted keys stored and managed by said APwireless access point, ~~to advise said STA of that effect;~~

said STAone of said plurality of wireless access terminal devices also comprising an updating unit updating an nth encrypted key stored and managed by said STAone of said plurality of wireless access terminal devices on reception of an nth encrypted key by delivered said ~~STA~~-encrypted key delivery message from said APwireless access point.

11. (Currently amended): The updating system for an encrypted key for a wireless LAN as defined in claim 1 wherein:

said STAone of said plurality of wireless access terminal devices comprises means for notifying the APwireless access point of a lumped ~~STA~~-encrypted key updating requesting message on detection of a preset factor;

said APwireless access point comprising means for notifying said ~~SV~~key management server device of ~~the lumped STA-encrypted key updating request on~~ reception of said lumped ~~STA~~-encrypted key updating requesting message from said STAone of said plurality of wireless access terminal devices;

said ~~SV~~key management server device comprising means for verifying whether or not the encrypted key addressed to said STAone of said plurality of wireless access terminal devices can be delivered in a lump to said STAone of said plurality of wireless access terminal devices on reception of said lumped ~~STA~~-encrypted key updating request from said APwireless access point; and

means for delivering encrypted key addressed to said ~~STA~~one of said plurality of wireless access terminal devices in lump to said ~~AP~~wireless access point if said verifying means has verified that the encrypted key can be delivered in a lump to said ~~STA~~one of said plurality of wireless access terminal devices;

said ~~AP~~wireless access point also comprising means for generating a lumped ~~STA~~-encrypted key delivery message on reception in lump of said encrypted keys addressed to said ~~STA~~one of said plurality of wireless access terminal devices from said ~~SV~~key management server device, and for notifying said ~~STA~~ of that effect;

said ~~STA~~one of said plurality of wireless access terminal devices also comprising means for updating the encrypted keys stored in said ~~STA~~one of said plurality of wireless access terminal devices in lump on reception of said lumped ~~STA~~-encrypted key delivery message from said ~~AP~~wireless access point.

12. (Currently amended): An updating method for an encrypted key for a wireless LAN comprising:

- (a) providing ~~one or more~~ wireless access ~~point~~points (APs) provided on a LAN, said ~~wireless access point~~APs being wirelessly connected to a ~~plurality of one or more~~ wireless access terminal devices (~~STAs~~) and in which data is encrypted and transmitted between the ~~AP~~wireless access point and the ~~STA or STAs~~plurality of wireless access terminal devices; to effect communication termed as “encrypted communication”;
- (b) generating, by a key management server (~~SV~~) device, LAN-connected to said ~~AP~~wireless access point, k encrypted keys, k being not less than 1,



used for encrypted communication between said ~~AP~~wireless access point and said ~~STA or STAs~~plurality of wireless access terminal devices;

- (c) storing and managing, by said ~~SV~~key management server device the ~~generated k~~ encrypted ~~keys~~key;
- (d) updating one of the encrypted ~~key~~keys under a preset condition, and
- (e) delivering the updated encrypted key to said ~~AP~~wireless access point and to said ~~STA or STAs~~plurality of wireless access terminal devices.

13. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 12 wherein:

said ~~SV~~key management server device in updating said k encrypted keys stored and managed by said ~~SV~~key management server updates said k encrypted keys at a rate of one at a time.

14. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 12 wherein:

said ~~SV~~key management server device in updating said k encrypted keys stored and managed by said ~~SV~~key management server device sequentially updates said k encrypted keys at a rate of one-by-one at a preset time interval.

15. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 12 wherein:

where k is greater than 1, said ~~SV~~key management server device sequentially updates all except a remaining one key (~~k-1~~) of said k encrypted keys stored in and managed by said ~~SV~~key management server device one-by-one at a first preset interval, said ~~SV~~key management server device

updating the remaining one key at a second interval longer than for said first preset interval( ~~$k-1$~~ ) ~~encrypted keys~~.

16. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 13 wherein:

said ~~AP~~wireless access point has encrypted communication with said ~~STA or STAs~~plurality of wireless access terminal devices using ~~another an optional~~ encrypted key other than ~~an~~the  $n$ th encrypted key stored in and managed by said ~~AP~~wireless access point, during a period of time since updating of the  $n$ th encrypted key stored in and managed by said ~~AP~~wireless access point until the another encrypted key is updated next, where  $1 \leq n \leq k$ .

17. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 13 wherein:

said ~~AP~~wireless access point has encrypted communication with said ~~STA or STAs~~plurality of wireless access terminal devices, sequentially using each one of  ~~$k(k-1)$~~  encrypted keys, other than ~~an~~the  $n$ th encrypted key stored in and managed by said ~~AP~~wireless access point, during a period of time since updating of the  $n$ th encrypted key stored in and managed by said ~~AP~~wireless access point until next updating of encrypted key, where  $1 \leq n \leq k$ .

18. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 13 wherein:

said ~~AP~~wireless access point has encrypted communication with said ~~STA or STAs~~plurality of wireless access terminal devices, using an initially updated one of  $k$  encrypted keys stored in and managed by said ~~AP~~wireless access point.

19. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 16 wherein:

said plurality of wireless access terminal devices encrypt~~STA or STAs~~ has/have  
encrypted communication with said ~~AP~~wireless access point, using an  
~~optional~~ one of ~~(k-1)~~said k encrypted keys, other than the nth  
encrypted key, stored in and managed by said ~~STA or STAs~~plurality of  
wireless access terminal devices.

20. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 16 wherein:

said plurality of wireless access terminal devices communicate~~STA or STAs~~  
~~has/have communication~~ with said ~~AP~~wireless access point, sequentially  
using each one of said k~~(k-1)~~ encrypted keys, other than the nth  
encrypted key, stored in and managed by said ~~STA or STAs~~plurality of  
wireless access terminal devices.

21. (Currently amended): The updating method for an encrypted key for a wireless LAN as defined in claim 16 wherein:

said plurality of wireless access terminal devices communicate~~STA or STAs~~  
~~has/have communication~~ with said ~~AP~~wireless access point, using the  
last updated one of k encrypted keys stored in and managed by said ~~STA~~  
~~or STAs~~plurality of wireless access terminal devices.

22. (New): An encryption key management system, comprising:

a key management server device, comprising:

an encryption key generating unit, and

an encryption key storage unit that stores  $k$  encryption keys  
generated by said encryption key generating unit;

a wireless access point coupled to said key management server device;  
and

a plurality of wireless access terminal devices wirelessly coupled to said  
wireless access point, each of said wireless access terminal devices  
storing said  $k$  encryption keys.

23. (New): The encryption key management system of claim 22, wherein one  
of said plurality of wireless access terminal devices generates and sends a  
request for a replacement key for one key of said plurality of encryption  
keys; and

wherein said key management server device sends a first message that is  
encrypted with another one of said plurality of encryption keys,  
said first message comprising said replacement key.

24. (New): The encryption key management system of claim 23, wherein said  
request comprises identifying information of said one of said plurality of  
wireless access terminal devices and wherein said key management server  
verifies said identifying information.

25. (New): The encryption key management system of claim 22, further  
comprising an open key encryption messaging protocol employed by  
said key management server device, said wireless access point, and said  
plurality of wireless access terminal devices, and wherein said key  
management server sends a second message comprising said plurality of  
encryption keys, and wherein said second message is encrypted by said  
open key encryption messaging protocol.